UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/553,920	10/20/2005	Thomas Andreas Maria Kevenaar	NL 030429	1357

24737 7590 08/06/2008
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
PATEL, JAY P	

ART UNIT	PAPER NUMBER
2619	

MAIL DATE	DELIVERY MODE
08/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/553,920	**Applicant(s)** KEVENAAR ET AL.	
	Examiner JAY P. PATEL	**Art Unit** 2619	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 October 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-9 and 11-16* is/are rejected.

7)☒ Claim(s) *5 and 10* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 October 2005* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 14-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

In regards to claim 14, it is directed to a signal which is non-statutory

In regards to claims 15 and 16, they are directed to a computer program product, which is non statutory.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 12 and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Munger et al. (US Patent 7133930 B2) further in view of Donahue (US Patent 7149219 B2).

3. In regards to claim 1, Munger shows in figure 11, an IP packet(s) (a first communication fragment) embedded into an Ethernet frame(s). The IP packets are inclusive of source and destination IP addresses (a first address reference) 1102A-B,

1103A-B and 1105A-B (since the IP addresses are present, they must be generated therefore Munger reads on generating at a first layer a first communication fragment comprising a first address reference referring to a first entity).

4. The Ethernet frame(s) in figure 11 from Munger (a second communication fragment) has source hardware addresses 1101A, 1104A (a second address reference referring a second entity which is related to the first entity; since the IP packet(s) are embedded in the Ethernet frame(s) the second entity (the hardware node) is related to the first entity (the entity with the IP address)). Since Ethernet frame(s) are present, they must be generated.

5. Figure 12A in Munger is an illustration of two nodes communicating over an Ethernet connection (A transmitting method of transmitting data using a layered communication model (please refer to the ISO stacks and software 1204 and 1217) and transmitting data comprising the second communication fragment).

6. Figure 2 in Munger is an illustration of a secure network inclusive of TARP routers and IP routers.

7. In further regards to claim 1 however, Munger fails to particularly teach the transmission method comprising the step of at least partially removing the first address reference in the transmitted data). Donahue however teaches removing an IP address of a node at step 742 in step 7B.

8. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the removal of an IP address as taught by Donahue into the secure communication system taught by Munger. The motivation to

do so would be to, hide the identity of the route that the packet has taken to reach its destination.

9. In regards to claim 12, Munger shows in figure 11, an IP packet(s) (a first communication fragment) embedded into an Ethernet frame(s). The IP packets are inclusive of source and destination IP addresses (a first address reference) 1102A-B, 1103A-B and 1105A-B (since the IP addresses are present, they must be generated therefore Munger reads on generating at a first layer a first communication fragment comprising a first address reference referring to a first entity).

10. The Ethernet frame(s) in figure 11 from Munger (a second communication fragment) has source hardware addresses 1101A, 1104A (a second address reference referring a second entity which is related to the first entity; since the IP packet(s) are embedded in the Ethernet frame(s) the second entity (the hardware node) is related to the first entity (the entity with the IP address)). Since Ethernet frame(s) are present, they must be generated.

11. Figure 12A in Munger is an illustration of two nodes communicating over an Ethernet connection (A transmitter device for transmitting data using a layered communication model (please refer to the ISO stacks and software 1204 and 1217) and transmitting data comprising the second communication fragment).

12. Figure 2 in Munger is an illustration of a secure network inclusive of TARP routers and IP routers.

13. In further regards to claim 12 however, Munger fails to particularly teach the transmission method comprising the step of at least partially removing the first address

reference in the transmitted data). Donahue however teaches removing an IP address of a node at step 742 in step 7B.

14. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the removal of an IP address as taught by Donahue into the secure communication system taught by Munger. The motivation to do so would be to, hide the identity of the route that the packet has taken to reach its destination.

15. In regards to claim 14, Munger shows in figure 11, an IP packet(s) (a first communication fragment) embedded into an Ethernet frame(s). The IP packets are inclusive of source and destination IP addresses (a first address reference) 1102A-B, 1103A-B and 1105A-B (since the IP addresses are present, they must be generated therefore Munger reads on generating at a first layer a first communication fragment comprising a first address reference referring to a first entity).

16. The Ethernet frame(s) in figure 11 from Munger (a second communication fragment) has source hardware addresses 1101A, 1104A (a second address reference referring a second entity which is related to the first entity; since the IP packet(s) are embedded in the Ethernet frame(s) the second entity (the hardware node) is related to the first entity (the entity with the IP address)). Since Ethernet frame(s) are present, they must be generated.

17. Figure 12A in Munger is an illustration of two nodes communicating over an Ethernet connection (A transmitting method of transmitting data using a layered

communication model (please refer to the ISO stacks and software 1204 and 1217) and transmitting data comprising the second communication fragment).

18. Figure 2 in Munger is an illustration of a secure network inclusive of TARP routers and IP routers.

19. In further regards to claim 14 however, Munger fails to particularly teach the transmission method comprising the step of at least partially removing the first address reference in the transmitted data). Donahue however teaches removing an IP address of a node at step 742 in step 7B.

20. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the removal of an IP address as taught by Donahue into the secure communication system taught by Munger. The motivation to do so would be to, hide the identity of the route that the packet has taken to reach its destination.

21. In regards to claim 15, Munger shows in figure 11, an IP packet(s) (a first communication fragment) embedded into an Ethernet frame(s). The IP packets are inclusive of source and destination IP addresses (a first address reference) 1102A-B, 1103A-B and 1105A-B (since the IP addresses are present, they must be generated therefore Munger reads on generating at a first layer a first communication fragment comprising a first address reference referring to a first entity).

22. The Ethernet frame(s) in figure 11 from Munger (a second communication fragment) has source hardware addresses 1101A, 1104A (a second address reference referring a second entity which is related to the first entity; since the IP packet(s) are

embedded in the Ethernet frame(s) the second entity (the hardware node) is related to the first entity (the entity with the IP address)). Since Ethernet frame(s) are present, they must be generated.

23. Figure 12A in Munger is an illustration of two nodes communicating over an Ethernet connection (A transmitter computer program product to implement communication using a layer communication model (please refer to the ISO stacks and software 1204 and 1217) and transmitting data comprising the second communication fragment).

24. Figure 2 in Munger is an illustration of a secure network inclusive of TARP routers and IP routers.

25. In further regards to claim 15 however, Munger fails to particularly teach the transmission method comprising the step of at least partially removing the first address reference in the transmitted data). Donahue however teaches removing an IP address of a node at step 742 in step 7B.

26. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the removal of an IP address as taught by Donahue into the secure communication system taught by Munger. The motivation to do so would be to, hide the identity of the route that the packet has taken to reach its destination.

27. Claims 6, 11, 13 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Munger et al. (US Patent 7133930 B2) in view of Donahue (US Patent 7149219 B2) further in view of Killcommons (US Patent 7028182 B1).

28. In regards to claim 6, Munger shows in figure 11, an IP packet(s) (a first communication fragment) embedded into an Ethernet frame(s) (the second communication fragment). The IP packets are inclusive of source and destination IP addresses (a first address reference) 1102A-B, 1103A-B and 1105A-B (since the IP addresses are present, they must be generated therefore Munger reads on generating at a first layer a first communication fragment comprising a first address reference referring to a first entity).

29. The Ethernet frame(s) in figure 11 from Munger (a second communication fragment) has source hardware addresses 1101A, 1104A (a second address reference referring a second entity which is related to a first entity being based on a first communication fragment comprising a first address reference to the first entity; since the IP packet(s) are embedded in the Ethernet frame(s) the second entity (the hardware node) is related to the first entity (the entity with the IP address)). Since Ethernet frame(s) are present, they must be generated.

30. Figure 12A in Munger is an illustration of two nodes communicating over an Ethernet connection (A receiving method of receiving data using a layered communication model (please refer to the ISO stacks and software 1204 and 1217) and retrieving the first communication fragment from the second communication fragment).

31. Figure 2 in Munger is an illustration of a secure network inclusive of TARP routers and IP routers.

32. In further regards to claim 6 however, Munger fails to particularly teach the transmission method comprising the step of at least partially removing the first address

reference in the transmitted data). Donahue however teaches removing an IP address of a node at step 742 in step 7B.

33. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the removal of an IP address as taught by Donahue into the secure communication system taught by Munger. The motivation to do so would be to, hide the identity of the route that the packet has taken to reach its destination.

34. In further regards to claim 6, neither Munger nor Donahue teach restoring the first address reference in retrieving the first communication fragment. Killcommons however teaches restoration of IP address (see column 9, lines 48-51).

35. Therefore, it would have been obvious to incorporate the restoration of the IP address as taught by Killcommons with the teachings of Donahue and Munger. The motivation to do so would be to prevent from registration of numerous IP addresses (see column 9 in Killcommons, lines 51-53).

36. In regards to claim 11, Munger shows in figure 11, an IP packet(s) (a first communication fragment) embedded into an Ethernet frame(s). The IP packets are inclusive of source and destination IP addresses (a first address reference) 1102A-B, 1103A-B and 1105A-B (since the IP addresses are present, they must be generated therefore Munger reads on generating at a first layer a first communication fragment comprising a first address reference referring to a first entity).

37. The Ethernet frame(s) in figure 11 from Munger (a second communication fragment) has source hardware addresses 1101A, 1104A (a second address reference

referring a second entity which is related to the first entity; since the IP packet(s) are embedded in the Ethernet frame(s) the second entity (the hardware node) is related to the first entity (the entity with the IP address)). Since Ethernet frame(s) are present, they must be generated.

38. Figure 12A in Munger is an illustration of two nodes communicating over an Ethernet connection (A transmitting method of transmitting data using a layered communication model (please refer to the ISO stacks and software 1204 and 1217) and transmitting data comprising the second communication fragment).

39. Figure 2 in Munger is an illustration of a secure network inclusive of TARP routers and IP routers.

40. The Ethernet frame(s) in figure 11 from Munger (a second communication fragment) has source hardware addresses 1101A, 1104A (a second address reference referring a second entity which is related to a first entity being based on a first communication fragment comprising a first address reference to the first entity; since the IP packet(s) are embedded in the Ethernet frame(s) the second entity (the hardware node) is related to the first entity (the entity with the IP address)). Since Ethernet frame(s) are present, they must be generated.

41. Figure 12A in Munger is an illustration of two nodes communicating over an Ethernet connection (A receiving means being arranged to receive data comprising the second communication fragment (please refer to the ISO stacks and software 1204 and 1217) and retrieving the first communication fragment from the second communication fragment).

42. Figure 2 in Munger is an illustration of a secure network inclusive of TARP routers and IP routers.

43. In further regards to claim 11 however, Munger fails to particularly teach the transmission method comprising the step of at least partially removing the first address reference in the transmitted data). Donahue however teaches removing an IP address of a node at step 742 in step 7B.

44. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the removal of an IP address as taught by Donahue into the secure communication system taught by Munger. The motivation to do so would be to, hide the identity of the route that the packet has taken to reach its destination.

45. In further regards to claim 11, neither Munger nor Donahue teach restoring the first address reference in retrieving the first communication fragment. Killcommons however teaches restoration of IP address (see column 9, lines 48-51).

46. Therefore, it would have been obvious to incorporate the restoration of the IP address as taught by Killcommons with the teachings of Donahue and Munger. The motivation to do so would be to prevent from registration of numerous IP addresses (see column 9 in Killcommons, lines 51-53).

47. In regards to claim 13, Munger shows in figure 11, an IP packet(s) (a first communication fragment) embedded into an Ethernet frame(s) (the second communication fragment). The IP packets are inclusive of source and destination IP addresses (a first address reference) 1102A-B, 1103A-B and 1105A-B (since the IP

addresses are present, they must be generated therefore Munger reads on generating at a first layer a first communication fragment comprising a first address reference referring to a first entity).

48. The Ethernet frame(s) in figure 11 from Munger (a second communication fragment) has source hardware addresses 1101A, 1104A (a second address reference referring a second entity which is related to a first entity being based on a first communication fragment comprising a first address reference to the first entity; since the IP packet(s) are embedded in the Ethernet frame(s) the second entity (the hardware node) is related to the first entity (the entity with the IP address)). Since Ethernet frame(s) are present, they must be generated.

49. Figure 12A in Munger is an illustration of two nodes communicating over an Ethernet connection (A receiving method of receiving data using a layered communication model (please refer to the ISO stacks and software 1204 and 1217) and retrieving the first communication fragment from the second communication fragment).

50. Figure 2 in Munger is an illustration of a secure network inclusive of TARP routers and IP routers.

51. In further regards to claim 13 however, Munger fails to particularly teach the transmission method comprising the step of at least partially removing the first address reference in the transmitted data). Donahue however teaches removing an IP address of a node at step 742 in step 7B.

52. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the removal of an IP address as taught by

Donahue into the secure communication system taught by Munger. The motivation to do so would be to, hide the identity of the route that the packet has taken to reach its destination.

53. In further regards to claim 13, neither Munger nor Donahue teach restoring the first address reference in retrieving the first communication fragment. Killcommons however teaches restoration of IP address (see column 9, lines 48-51).

54. Therefore, it would have been obvious to incorporate the restoration of the IP address as taught by Killcommons with the teachings of Donahue and Munger. The motivation to do so would be to prevent from registration of numerous IP addresses (see column 9 in Killcommons, lines 51-53).

55. In regards to claim 16, Munger shows in figure 11, an IP packet(s) (a first communication fragment) embedded into an Ethernet frame(s) (the second communication fragment). The IP packets are inclusive of source and destination IP addresses (a first address reference) 1102A-B, 1103A-B and 1105A-B (since the IP addresses are present, they must be generated therefore Munger reads on generating at a first layer a first communication fragment comprising a first address reference referring to a first entity).

56. The Ethernet frame(s) in figure 11 from Munger (a second communication fragment) has source hardware addresses 1101A, 1104A (a second address reference referring a second entity which is related to a first entity being based on a first communication fragment comprising a first address reference to the first entity; since the IP packet(s) are embedded in the Ethernet frame(s) the second entity (the hardware

node) is related to the first entity (the entity with the IP address)). Since Ethernet frame(s) are present, they must be generated.

57. Figure 12A in Munger is an illustration of two nodes communicating over an Ethernet connection (A receiver computer program to implement communication using a layered communication model (please refer to the ISO stacks and software 1204 and 1217) and retrieving the first communication fragment from the second communication fragment).

58. Figure 2 in Munger is an illustration of a secure network inclusive of TARP routers and IP routers.

59. In further regards to claim 16 however, Munger fails to particularly teach the transmission method comprising the step of at least partially removing the first address reference in the transmitted data). Donahue however teaches removing an IP address of a node at step 742 in step 7B.

60. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the removal of an IP address as taught by Donahue into the secure communication system taught by Munger. The motivation to do so would be to, hide the identity of the route that the packet has taken to reach its destination.

61. In further regards to claim 16, neither Munger nor Donahue teach restoring the first address reference in retrieving the first communication fragment. Killcommons however teaches restoration of IP address (see column 9, lines 48-51).

62. Therefore, it would have been obvious to incorporate the restoration of the IP address as taught by Killcommons with the teachings of Donahue and Munger. The motivation to do so would be to prevent from registration of numerous IP addresses (see column 9 in Killcommons, lines 51-53).

63. Claims 2-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Munger et al. (US Patent 7133930 B2) in view of Donahue (US Patent 7149219 B2) further in view of Krause et al. (US Patent 6070198).

64. In regards to claims 2-4, Munger and Donahue fail to teach using a cryptographic protection before the first address reference is removed and that it is provided only at the single layer where the message was initiated. Krause however, teaches the above-mentioned limitation.

65. Krause teaches using a cryptographic strategy for all data going through a TCP/IP stack, independent of any user applications (thus being implement at the TCP/IP layer independent of the higher layers) that may use the TCP/IP stack (see column 16, lines 53-58).

66. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the cryptographic strategy as taught by Krause into the teachings of Munger and Donahue. The motivation to do so would be provide security and to enable robust decryption that is also not complicated by multiple layers of encryption.

67. Claims 7-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Munger et al. (US Patent 7133930 B2) in view of Donahue (US Patent 7149219 B2)

further in view of Killcommons (US Patent 7028182 B1) further in view of Krause et al. (US Patent 6070198).

68. In regards to claims 7-9, Munger, Donahue and Killcommons fail to teach using a cryptographic protection before the first address reference is removed and that it is provided only at the single layer where the message was initiated. Krause however, teaches the above-mentioned limitation.

69. Krause teaches using a cryptographic strategy for all data going through a TCP/IP stack, independent of any user applications (thus being implement at the TCP/IP layer independent of the higher layers) that may use the TCP/IP stack (see column 16, lines 53-58).

70. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the cryptographic strategy as taught by Krause into the teachings of Munger, Donahue and Killcommons. The motivation to do so would be provide security and to enable robust decryption that is also not complicated by multiple layers of encryption.

Allowable Subject Matter

71. Claims 5 and 10 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

72. In regards to claims 5 and 10, the cited prior art fails to teach, either individually or in combination, replacing the first address reference with the second address reference. The closest prior art Ma et al. (US Patent 6856591 B1) teaches, replacing an

IP address with a virtual IP address and replacing a MAC address with a virtual MAC address (see column 11, lines 25-29).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAY P. PATEL whose telephone number is (571)272-3086. The examiner can normally be reached on M-F 9:00 am - 5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jay P. Patel
Examiner
Art Unit 2619

/J. P. P./
Examiner, Art Unit 2619

/Hassan Kizou/
Supervisory Patent Examiner, Art Unit 2619